HWAM Capability Data Sheet

Desired State:

- Only **devices** in the authorized **Hardware Inventory** are on the network
- All authorized devices are in the authorized hardware inventory
- All authorized devices are assigned to a manager

Desired State Specification Data Requirements:

Data Item:	Justification:
Data necessary to accurately identify the device. At a minimum: • Serial Number • Expected CPE for hardware or equivalent ○ Vendor ○ Product ○ Model Number • Static IP Address (where applicable) • Media Access Control (MAC) Address • Property Number Local enhancements[1] might include data necessary to accurately identify subcomponents	To be able to uniquely identify the device. To be able to validate that the device on the network is the device authorized, and not an "imposter."
Data necessary to describe a device such that other capabilities can determine the appropriate defect checks to run on that device. • Expected CPE for operating system of device or equivalent ○ Vendor ○ Product ○ Version ○ Release level	To ensure all appropriate defects for a device are defined, run, and reported. To help identify non-reporting associated with other capabilities that look for defects on the device.

[1] Departments and Agencies can define data requirements and associated defects for their local environment. This is done in coordination with the CMaaS contractor and these local defects are not reported to the Federal Dashboard.

Data Item:	Justification:
A person or organization that is responsible for managing the device (note: this should be a reasonable assignment, do not count management assignments where a person or organization is assigned too many devices to effectively manage them). Local enhancements might include: • Approvers being assigned • Managers being approved • Managers acknowledging receipt	To know who to instruct to fix specific risk conditions found. To assess each such persons performance in risk management.
Data necessary to compare devices discovered on the network to the authorized hardware inventory. Site dependent, examples include • IP address • MAC address • Host-based certificate or Agent ID • Device domain name	To be able to identify unauthorized devices. To know which devices have defects.
Data necessary to locate a physical device.	To ensure that managers can find the device to: • Revalidate it for supply chain risk management. • Remove it if unauthorized
The period of time the device is authorized Local enhancements might include: • When the device must be physically inspected/verified for supply chain risk management	To allow previously authorized devices to remain in the authorized hardware inventory, but know they are no longer authorized.
Expected status of the device (e.g, authorized, expired, pending approval, missing) to include: • Date first authorized • Date of most recent authorization • Date authorization revoked Local enhancements might include: • Returned from high-risk location • Removed pending reauthorization • Date of last status change	To determine which devices in the authorized hardware inventory are not likely to be found in actual state inventory.

Actual State:

- Devices identified as connected to the network
- Sensors and/or process to detect and record/report actual inventory

Actual State Data Requirements:

While not explicitly stated below, all Actual State Data elements must have a date/time associated with each collection instance of that element[2].

Data Item:	Justification:
Data necessary to accurately identify the device. Site specific, examples include: • IP Address • MAC Address • Host-based certificate or Agent ID • Device domain name	To be able to assert which operational device is unauthorized, or has some other defect.
Data necessary to describe the attributes of a device such that other capabilities can determine the appropriate defect checks to run on that device. • Expected CPE for operating system of device or equivalent ○ Vendor ○ Product ○ Version ○ Release level	To ensure all appropriate defects for these devices are defined, run, and reported.
Data necessary to compare devices connected to the network to the authorized hardware inventory. • IP Address and associated logs • MAC Address • Host-based certificate or Agent ID • Device domain name	To be able to identify unauthorized devices.
Data necessary to locate physical assets based on information collected in the operational environment. Site specific, examples include: • Edge switch that detected device • Host that USB drive was connected to	To ensure that managers can find the device to fix, validate, or remove it.
Data necessary to determine how long devices have been present in the environment. At a minimum: - Date/time it was first discovered - Date/time it was last seen	To determine how long the device has been in existence and the last time it was detected in the enterprise

[2] Collection often occurs in batches, where the sensors collect from a set of devices at once. As long as a date/time can be provided for the data resulting from that collection to a reasonable precision (i.e., ± 1 hour), that is acceptable.

Defects:

A defect is a difference between the information in the authorized hardware inventory and either what is required to be in the authorized inventory or what is in the actual inventory. Defects are sent to the dashboard and scored.

Defect Type.	Why is this considered a risk condition?	Typical Mitigation[3] Option 1:	Typical Mitigation Option 2:
A device is in the actual state inventory, but NOT in the authorized hardware inventory	The device is unauthorized. We are unable to determine if device is authorized.	If the device should be operating in the environment, authorize it, add it to authorized hardware inventory, and assign it for management.	Otherwise, remove the device from the environment.
A device is in the authorized hardware inventory and the actual inventory, but no one is assigned to manage it Local enhancements might include: • Manager has not accepted responsibility • Manager has not been approved	The asset Manager is unknown.	If management has already been assigned, identify the manager and record the result in authorized hardware inventory.	Otherwise, assign the device to an appropriate manager and record this in authorized hardware inventory. (As a result this manager will be informed of other risk conditions on the device so they can be addressed.)

[3] Risk acceptance is always an option. In the case of Option 1 and Option 2, the risk conditions and scores do not go away. They remain visible to ensure that the organization understands the impact of their risk acceptance decisions over time and in aggregate.

Defect Type.	Why is this considered a risk condition?	Typical Mitigation[3] Option 1:	Typical Mitigation Option 2:
A device is in the authorized hardware inventory, but not in actual inventory. The status in the authorized hardware inventory does not provide a reason for not being in the actual inventory	The device may not be reporting, which would reduce our ability to monitor it in other areas. The device may have been accidentally or maliciously removed from the operational environment (e.g., missing or lost). The device may have been intentionally removed from the environment for security reasons.	If the device is actually operational but not reporting, this is a possible sensor problem. Work with the sensor managers to troubleshoot problem.	Otherwise, the device may have been intentionally, accidentally, or maliciously removed from the environment. Investigate the cause. If the removal creates a security violation, record as an incident, and update the device status in the authorized hardware inventory. If the removal was for security purposes, either remove the device from the authorized hardware inventory or change the status reflect that it is not currently authorized to ensure you can detect unauthorized (re)use of the device.
A device is in both the authorized hardware and actual inventories, but the authorization is expired	The risk associated with authorization decisions increases with time. Decisions that were acceptable in the past may now be considered too risky.	If the device should be reauthorized for operation in the environment, make sure the status is set to authorized and reset the expiration date in the authorized hardware inventory.	Otherwise, remove the device from the authorized hardware inventory and the environment.
An important data element of the authorized hardware inventory is missing • CPE or equivalent	A key piece of information used to score or assign risk is unknown.	If the data element is known, record the information in the authorized hardware inventory.	Otherwise, determine or define the data element and record this in the authorized hardware inventory.
Locally defined defects where a required local	Visibility into specific vulnerable conditions	If the device is actually operational,	Otherwise, this is a possible

Defect Type.	Why is this considered a risk condition?	Typical Mitigation[3] Option 1:	Typical Mitigation Option 2:
condition is not checked on an associated device within a set timeframe. Examples include: • Device is not physically revalidated as the authorized device within the defined timeframe. • Non reporting devices not physically located within a set timeframe	of interest to the local enterprise is limited.	being sensed/processed, but not reporting/not having results reported for a particular condition, it is possible that there is incorrect data in the authorized hardware inventory. Update the authorized hardware inventory.	sensor/collection problem for automated checks and process problem for manual checks. Work with the sensor/collection managers or process owners to troubleshoot problem.

Appendix A - Definitions

Term	**Definition**
Authorized Hardware Inventory List	List of authorized hardware assets for an organization or subnet.
Black List	Banned list of assets for an organization or subnet.
Defect	A condition where the Desired State specification and the Actual State do not match in a manner that incurs risk to the organization.
Device	IP-addressable asset on the network or a non-addressable component (e.g. removable media) able to interact with the organization's data and resources.
Device Role	An enterprise-wide label for a class of devices that perform a like function in the environment. Examples are file servers, external web server, or workstation. The device role is intended to simplify assigning asset values or scoring weights by allowing D/As to define them for groups of devices and having individual devices inherit the values.
Hardware Asset Management (HWAM) Capability	The Continuous Diagnostic and Mitigation (CDM) capability that ensure unauthorized and/or unmanaged hardware is removed from the organization's network, or authorized and assigned for management, before it is exploited, compromising confidentiality, integrity, and/or availability.
Removable media	Removable storage devices that can be attached to a hardware asset on a network, typically by USB ports.
Scoring	The process of calculating the risk points for a defect. Identified defects will be "scored" based on the amount of perceived risk they create. The CDM program will be providing a scoring system that is generic across D/As. Each D/A may adapt this with additional D/A specific information to better prioritize defects for action.
White List	Approved list of assets for an organization or subnet.